

# Performance Evaluation of the DNP3 Protocol for Smart Grid Applications over IEEE 802.3/802.11 Networks and Heterogeneous Traffic

Alcides Ortega, Ailton A. Shinoda, Christiane M. Schweitzer, Fabrizio Granelli, Aleciana V. Ortega, and Fabiola Bonvecchio

**Abstract**—The Distributed Network Protocol Version 3.0 (DNP3) is a communications protocol used between components of a power grid system. DNP3 is designed to operate in network scenarios with high node density and can be used for both wired and wireless communications. Recently, with the evolution of power grid systems towards the smart grid, the use of DNP3 has been proposed for smart grid applications. Unfortunately, there exist few studies that evaluate the performance of DNP3 by means of computer-based simulations based on open-source software. Therefore, this paper proposes an evaluation of the performance of DNP3 over a mixed (wired/wireless) network between IEEE 802.3 and IEEE 802.11b, encapsulated over TCP/IP, using the Network Simulator Version 2.35 (NS-2). The purpose of the paper is to investigate the feasibility of using DNP3 over a network carrying heterogeneous traffic, such as monitoring and teleprotection, by measuring the delay required to complete a messaging operation. The simulation results show that DNP3 represents a feasible communications protocol for smart grid applications, which achieves delays shorter than 12 ms for teleprotection and below 90 ms for monitoring.

**Keywords**—IEEE 802.3, IEEE 802.11b, IEEE 1815 DNP3, NS-2, Simulator, Smart Grid.

## I. INTRODUCTION

THE smart grid is a new concept that combines enhanced power grid systems and advanced techniques of Information and Communication Technologies (ICT) to monitor and manage the transport of electricity from distribution substations of utilities to end consumers in real time [1].

Communications in the smart grid architecture are fundamental as they involve many actions of control and monitoring, for the proper operation of the electric systems [2]. Such communications are performed through a telecommunications infrastructure that can mainly be

This work had the financial support of the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP, 2014/06022-9) and Universidade Estadual de Mato Grosso do Sul (UEMS).

Alcides Ortega, Ailton A. Shinoda, Christiane M. Schweitzer, Aleciana V. Ortega is with UNESP, Campus Ilha Solteira, SP Brasil (e-mail: ortega.tex@gmail.com, shinoda@dee.feis.unesp.br, chris@mat.feis.unesp.br, aleciana@gmail.com).

Fabrizio Granelli is with DISI, University of Trento, Italy (e-mail: granelli@disi.unitn.it).

Fabiola Bonvecchio is with University of Leoben, Austria (e-mail: fabiola.bonvecchio@stud.unileoben.ac.at).

composed of wired and wireless communications systems [3].

The choice of wired and/or wireless communications by the utilities is based on various factors, such as geographic characteristics of the area of deployment and deployment and operational costs [4]. For instance, the uses of wireless communications in the smart grid system provide a lower cost and speed of deployment and portability when compared to wired communications. In this sense, wireless communications have been applied to sensors, IEDs (Intelligent Electronic Derive) and RTUs (Remote Terminal Unit) [5], [6].

A communications protocol that has recently been considered for smart grid applications and can be used for both wired and wireless communications is the IEEE 1815 DNP3 [7]. This is an open protocol for control and monitoring of the electric components of a power grid system. The DNP3 protocol is non-proprietary and standardized and optimized for low communication overhead, being one of the most widely used in the world, especially in North America, Latin America, Asia and Australia. The reasons for such wide adoption of DNP3 are due to its high security, interoperability, and adaptation to different applications, such as electric power substation automation, water plants treatment, and sewage, oil and gas system [8], [12].

The performance of DNP3 for smart grid applications has been evaluated in several studies. For instance, a real-setting testbed for research was developed and described in [9] to measure the messages delivery delay in a mixed communication of DNP3 over Transport Control Protocol/Internet Protocol (TCP/IP). Experimental results showed that DNP3 is in line with the requirements of the relay protection. Also, the authors claimed that DNP3 over TCP/IP is a suitable solution for real-time monitoring applications. However, it shows performance limitations to support time-critical applications.

Since experimental research for the smart grid requires a deep knowledge of hardware programming and a strong investment in hardware equipment to set up a real-setting scenario, most of works on the performance evaluation of DNP3 have been based on computer-based simulations. Unfortunately, these works employ licensed software, which does not allow new implementations or add new functions by non-proprietary partners in order to perform a simulation of DNP3 in a more realistic scenario of smart grid. Since licensed software is expensive and only proprietary partners can accomplish the update of new features, open-source software has been widely used for many years to conduct research in

both academia and research communities.

The NS-2 is a widely used open-source simulation framework that has been implemented and improved with the cooperation of many partners during many years. NS-2 allows abstraction of all communication protocols and their performance evaluation for different network topologies and configuration of various network traffic types.

In our previous work presented in [10], we evaluated the performance of DNP3 in an IEEE 802.3 Ethernet network encapsulated over TCP/IP by means of computer-based simulations using NS-2. Since NS-2 is based on open-source software, it allowed us to implement a new framework (or patch in the NS-2 terminology) in order to test the main functions of DNP3 in several scenarios. The functions that can be evaluated through simulations in NS-2 are: message request from a master station of outstations, transmission and retransmission of unsolicited messages sent from outstations, transmission and retransmission of unsolicited messages with read function, transmission and retransmission of unsolicited messages with different function of reading and transmission and retransmission restart command of outstations.

In this paper, we extend the work presented in [11] by evaluating the performance of DNP3 in a smart grid scenario composed of both wired and wireless communications systems using the IEEE 802.3 and IEEE 802.11b Standards, respectively, with. The simulated scenario considered for the work presented in this paper integrates heterogeneous traffic for monitoring and teleprotection applications, containing DNP3 packets and TCP packets, to verify analyze the performance as the number of retransmissions for packet loss and latency threshold, in which it was found that used in a wired network the DNP3 works well for monitoring applications, up to the limit of use of 85% of the bandwidth of a network and above this percentage without quality of service is unfeasible because the packet lost, re-transmissions and latency are significantly increased.

#### A. Simulation Model

A new scenario was considered to perform the Simulation of a heterogeneous network using wired networks and wireless, through the results of this Simulation will be possible to analyze the performance of the operation of the DNP3 in a scenario involving a control center and two substations of power electric distribution.

The configuration of this scenario are the following: the first substation is located to 22,8km of the control center, while the second is located to 21,3km and in both there is a base station that connects to the control center via the wired technology. In the first substation there are five outstations being that of them four use the wireless communication with the base station and one with wired, in the second substation there are four outstations being that three of which use wireless communication with the station base and one with wired.

In the first simulation was held the transmission of data packets of DNP3 only and in the second part of the simulation to evaluate both the performance of DNP3 in a mixed data traffic, with the results will be possible to analyze the

possibility of use on the same network and packet transmission DNP3 with other packet and use the network more efficiently.

This work is organized into sections. Section II presents the DNP3 Protocol. The simulations and their results in throughput, delay, are described in section III. Finally, section IV presents the conclusions.

## II. DNP3 PROTOCOL

The DNP3 is an open communication protocol and optimized developed for the SCADA (Supervisory Control and Data Acquisition) that is used to communicate among power grid equipment, with two classes of devices defined. Central stations (Masters) are usually devices with some processing power and data storage. Slave stations (Outstation) are devices located in field (transmission lines, transformer substations) to collect data from sensors and send the central station [13].

DNP3 protocol was initially designed to operate in traditional power grid and through the serial links. Recently, with the migration from traditional power grid to power grid systems, the reuse of existing communication protocols is widely regarded as a solution to cost-efficient and compatible with previous versions, and how the DNP3 does not specify its own network and lower layers, the DNP3 protocol over TCP/IP has been proposed as a communication protocol for smart grid, because is designed to be as robust as possible in regards to detecting and recovering from error [12]. DNP3 can be used in all kinds of communication be it wireless or wired [7].

#### A. Protocol Topology

The DNP3 standard defines four types of architecture:

Point to point: it is the simplest architecture, wherein a Master station communicates with a single remote station (Outstation).

Multipoint: a central station communicates with several slave stations. The communications for data requests are performed between the central station and each slave station in sequential mode. Each slave station monitors the messages from the central station and only responds when the destination address of the received message matches its address.

Hierarchical: it consists of a master that communicates with a slave station that in turn becomes a central station of another station. In this case, the second slave station gets its name from the central substation or Submaster.

Data concentrator: this topology can handle different protocols where the DNP3 may be running in a central station or in a central substation. The data concentrator collects information from various IEDs to be transmitted to the central station [7].

## III. RESULTS AND DISCUSSIONS

In this section we introduce the test scenario used in this paper and the setup of our simulations and discussions of the results.

Simulation Environment: Simulations are carried out in the

open-source network simulator NS-2 version 2.35 compiled into Fedora Core Linux operating system.

Traffic model: the DNP3 traffic generator with 292 bytes of information encapsulated in TCP/IP protocol, are added to the 20 bytes of the TCP header and 20 bytes of IP header totaling a data packet of 332 bytes, sent every 2 s of slave stations (outstations) to the master station and a data packet with confirmation of receipt sent to the master station to the outstation to the size of 40 bytes, the function of the DNP3 protocol used was the sending unsolicited messages, this function and used in DNP3 for when there is any change of state in any monitored equipment is automatically sent to the control center, are also used generator traffic TCP with packet size of 1040 bytes and 40 bytes are confirmation that the TCP ACK. The TCP traffic was used for simulating the utilization of FTP (File Transfer Protocol) that are used for file transfer rate between computers.

Simulation Scenarios: In this job we present the communication between the substations of distribution of electric power to the control center. The substations are located generally in the entrance of cities and the control center within the town, the Fig. 1 shows the scenario with two substations for the distribution of electric power and a control center, the first substation are five node, four node are IEDs (outstation) and one node representing a data server, three of the four outstation communicate with a base station (BS) via wireless and one via wired, communication data server and wireless too.

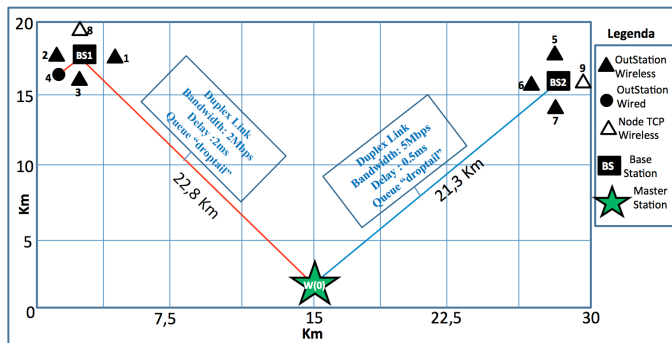


Fig. 1 Simulation scenario.

Communication with the BS and control center located 22,8 km and through wired, while the second substation is located 21,3 km from central control, this substation there is a BS connected via wireless with three outstations and a data server. Our goal was to make the time measurements of latency and amount of data packets retransmitted the DNP3 protocol in a mixed network consisting of 802.3 and 802.11b network from outstations to the master station at the control center in the second experiment we used the same scenario but with the traffic of heterogeneous data packets containing TCP and DNP3 data in order to check the latency time and the amount of lost packets.

Table I presents the configuration and composition of the simulated network topology, as well as the distance and the type of network interface connection used between the node and the BS, type of queue and packet traffic. The central station is connected to the gateway W(0), the communication

of the nodes to the gateway are performed through the BS. In this Table the outstation are the IEDs and the nodes are the data server, the topology of the network and connections.

On NS-2 all transport protocols are defined through an agent. In Fig. 1, using the parameters of Table I, have seven agents defined in outstations: TCP/SimpleTcp, two agents TCP/Newreno defined on node8 and node9 and two TCPSink defined in node W(0).

TABLE I- ASSUMED NETWORK PARAMETERS BETWEEN NODE AND BS.

Node	Network Interface	BS	Distance	Traffic	Queue
Outstation1	Wireless	1	300 m	DNP3	Droptail
Outstation2	Wireless	1	200 m	DNP3	Droptail
Outstation3	Wireless	1	200 m	DNP3	Droptail
Outstation4	Wired	1	10 m	DNP3	Droptail
Outstation5	Wireless	2	300 m	DNP3	Droptail
Outstation6	Wireless	2	200 m	DNP3	Droptail
Outstation7	Wireless	2	100 m	DNP3	Droptail
Node8	Wireless	1	300 m	FTP	Droptail
Node9	Wireless	2	300 m	FTP	Droptail

In this simulation was used the proactive DSDV (Destination Sequenced Distance Vector) Protocol maintains a table of possible routes for packet traffic throughout the network, all nodes employ wireless DSDV Protocol. In the Table II presents the configuration assumed between the connection of the BS at node w(0), as the type of traffic, queue, distance, latency, packet traffic and bandwidth.

TABLE II- ASSUMED NETWORK PARAMETERS BETWEEN BS AND GW.

BS	Duplex Link	Latency	Distance	Traffic	Queue	Gateway
1	2 Mb	2 ms	22,8 Km	DNP3 FTP	Droptail	W(0)
2	5 Mb	0,5 ms	21,3 Km	DNP3 FTP	Droptail	W(0)

Table III presents the main parameters of the considered network model in simulation of heterogeneous packet transmission, in the range of the gateway W(0) to the BS, and BS until wireless nodes.

Simulation of TCP application: TCP agent attached to the node W(0) and another agent of reception (Sink) linked to wireless Node8 and Node9. In addition, the associated application between the node W(0) and the wireless node Node8 and Node9 is the FTP. Agent Sink receives the TCP packets and generates recognition packages ACKs.

The advantage of TCP for applications is the versatility and robustness of this protocol, making it suitable to global networks, since it verifies that the data is sent correctly, in the proper sequence and no mistakes over the network, ensuring the transmission of packets.

One of the most well known uses of TCP protocol is cyber applications, such as SSH (Secure Shell), FTP, HTTP (Hyper Text Transfer Protocol), among others.

TABLE III - MODELED NETWORK PARAMETERS.

Parameter	Value
Channel	WirelessChannel
Propagation	TwoRayGround
Network interface	Wireless Phy
MAC layer	802.11
Queue type	DropTail
Link layer	LL
Model antenna	OmniAntenna
Maximum packet in the queue	60
Number of wireless nodes	8
Base Station	2
Number of wired node	2
Routing protocol	DSDV
Coverage area (XxY)	20km x 30km
Frequency	2.4 Ghz
Transmission rate	11Mb
Packet size	292, 1040 bytes
Type of application	DNP3, TCP
Event	Unsolicited messages

Simulation of DNP3 application: In Fig. 2 are illustrated the node and the agents (TCP/SimpleTcp) and application (TCPAppmod) linked in each node to perform the simulation of DNP3 in NS-2.

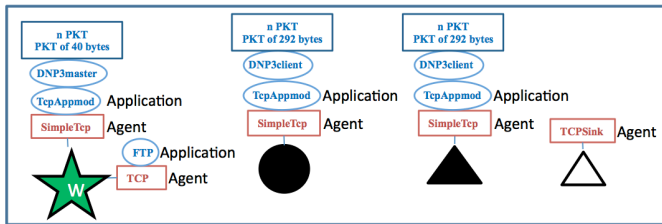


Fig. 2 Agents and applications running on each node type in DNP3 in NS-2.

The DNP3master receives the DNP3 protocol packets and after acknowledgment the TCPAppmod generates the DNP3 recognition packages with the size of 40 bytes. The advantage of this patch with the TCPAppmod for applications is the versatility and safety, making it suitable for global networks, since it verifies that the data is sent correctly and in the proper sequence with a specified time for receipt of the confirmation packages.

Table IV presents the time requirements to delay delivery of a message according to each type of application on the smart grid system.

TABLE IV – REQUIREMENTS OF MESSAGE DELIVERY DELAY [14].

Type	Delivery Delay	Application
Protection	3 ~ 16 ms	Trip, Closing, Reclosing.
Real-time monitoring	16 ~ 100 ms	State reporting
Low speed	≥ 100 ms	File transferring

Simulation result of throughput of the transmission of the DNP3 packet: Fig. 3 shows the flow of packets transmitted from Outstation1 to Outstation7 for the Master station. With the network parameters of Table I to Table III applied to the scenario of Fig. 1, the DNP3 traffic is generated every 2 s with a packet size of 292 bytes encapsulated in TCP/IP protocol, totaling 332 bytes of the packet transmitted, the yield expected average is about 166 bytes/sec (0,166 Kbytes/s).

The graph shown in Fig. 3 in which the Y axis shows the

throughput in Kbytes/s and the X axis simulation time in seconds, we note that there is no variation of throughput of packets with the same trafficking in heterogeneous packets, keeping the same throughput rate of (0,166 Kbytes/s), all the outstation of the station master, was generated a thousand packet were in each outstations, and the master station received a total of 7000 packets, the throughput is constant in simulation.

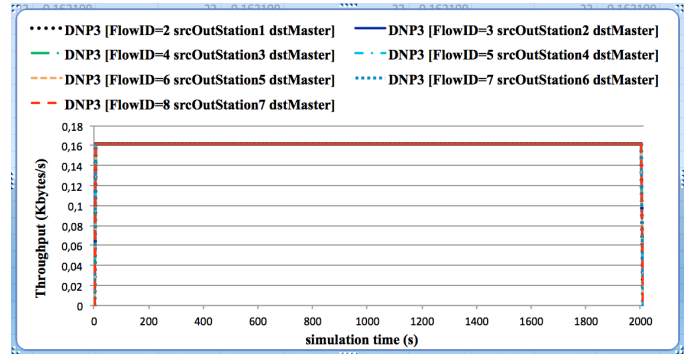


Fig. 3. Average flow of the seven statistical Outstation.

Fig. 4 illustrates the DNP3 delivery traffic delay of outstation to the master station by the BS1. The greater distance between the outstations and the master station is illustrated in Fig. 1 and specified in the Table I, the outstation which is farthest from the BS1 is the outstation1 with 300m and with the lowest distance is the outstation4 with 10m, noting that the outstation1 uses wireless technology and the outstation4 wired.

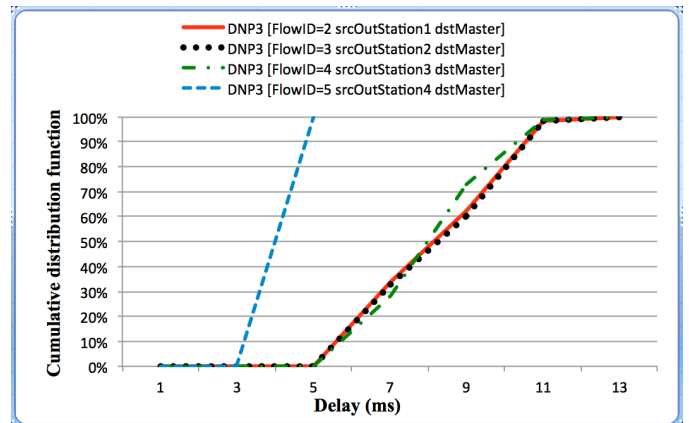


Fig. 4 Delay of Outstations from BS1 without TCP traffic.

The expected result was that the delay time of the outstation4 would be the lesser of the other outstation, because besides stay nearest and wired, and the graph show exactly this expected result. Analyzing the results of the graphics with the normal traffic of DNP3 without the FTP traffic, the results demonstrate that there was a perceptible difference between the outstation with wired and wireless, but between wireless outstations there was not perceptible differences in delay time, even with one difference in distances between them.

The results obtained through the cumulative distribution function (CDF) in a sample of 1000 packets, demonstrated through the graph curves that the trend is that packets sent by outstations with wired network and those who are closest to

BS1 and not using one heterogeneous network has the lowest delay time. The graphs illustrate the results exactly than 90% of the total sent packets from the outstation4 has the lower time delay longer than 5 ms.

While the other outstations using wireless networks to communicate with the BS1 and then wired up to the master station has a longer delay time in relation to wired outstation in graphic can be observed that 90% of the total packets sent from outstation1 to outstation3 has the time delay greater than 5 ms and less than or equal to 11 ms.

Fig. 5 illustrates the delay in delivery of the DNP3 traffic of outstation to the Master station via the BS2. The distance between the outstation's and the Master station, the greater distance is between the outstation5 until the BS2, nearest the BS2 is the outstation7 with 100 m.

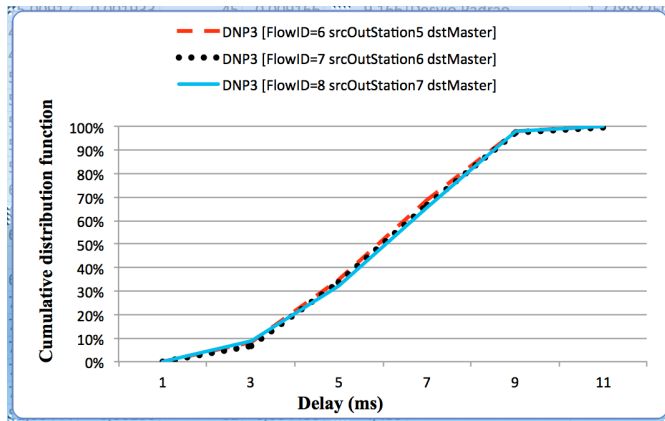


Fig. 5 Delay of Outstations from BS2 without TCP traffic.

The results obtained through the CDF in a sample of 1000 packets demonstrate through the curves that the trend is that packets sent by outstations are more alike and with few differences, in General 90% of packets sent has a delay less than 9 ms.

Fig. 6 shows the comparison of the average statistical throughput or instantaneous flow (measured at each 1 s) of packets transmitted from node wired W(0) to BS. This, in turn, makes the routing of packets to the Node8 and Node9 of the TCP, the simulation for both began the 2 s and finished in 2004 s.

The graph presents the result of simulations of TCP traffic, the black line identified in the graph and the result of the flow of TCP traffic from Node8 to the BS1 and BS1 until the Gateway W(0) with a transfer rate of 540 Kb. It should be noted that the average flow of the TCP traffic from BS1 was 240 Kbytes/s and no changes TCP traffic already identified with the color blue.

A result of the TCP traffic throughput from Node9 to the BS2 and the BS2 until the Gateway W(0), also with a transfer rate of 512 Kb. It should be noted that the average throughput of the TCP traffic from sub BS2 was 275 Kbytes/s and with few fluctuations during the simulation due to discard packets.

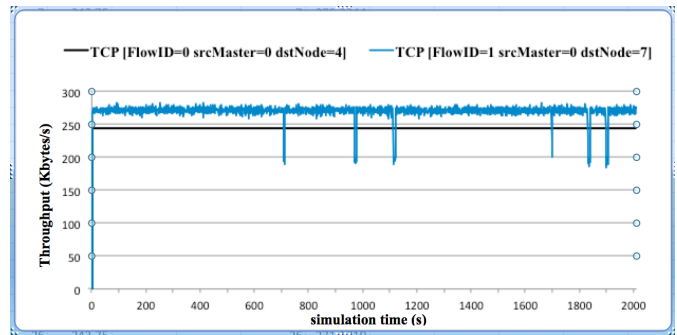


Fig. 6 Average throughput statistic of TCP traffic.

The results showed that using the TCP transport protocol and DSDV routing protocol, the packages were led with an average and instantaneous throughput almost constant for the wireless network, and node8 with a few variations along the node9 simulation.

Fig. 7 illustrates the delay in delivery of the DNP3 traffic of outstation to the Master via the BS1 with TCP traffic with a 512 Kb rate. Note that the outstation4 who obtained 90% of packages delivered less than 4 ms with TCP traffic crossed the 4 ms to 77 ms.

The others which obtained the time of delay in the delivery of packages with 90% less than or equal to 10 ms passed for 91 ms. with the result of simulations with TCP traffic, the delay time only serves to real-time monitoring as well as for data acquisition from sensors that are not employed to teleprotection, because in this case the maximum delay time allowed is up to 16 ms.

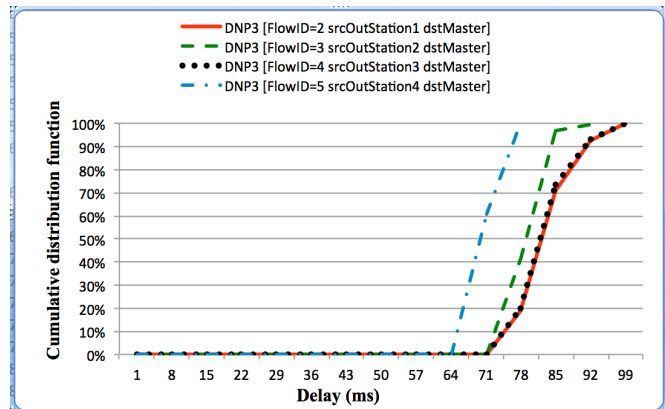


Fig. 7 Delay of Outstations of BS1 with TCP traffic.

Fig. 8 illustrates the delay in delivery of the DNP3 traffic of outstation to the Master station by the BS2 with the introduction of the TCP traffic.

Note that the results, obtained previously with 90% of packages delivered and confirmed with a shorter 9 ms, passed to 75 ms in/from the outstation8 that is the closest to the BS2, others passed 84 ms. The results of the simulations demonstrate that with the TCP traffic is possible DNP3 communication for real-time monitoring.



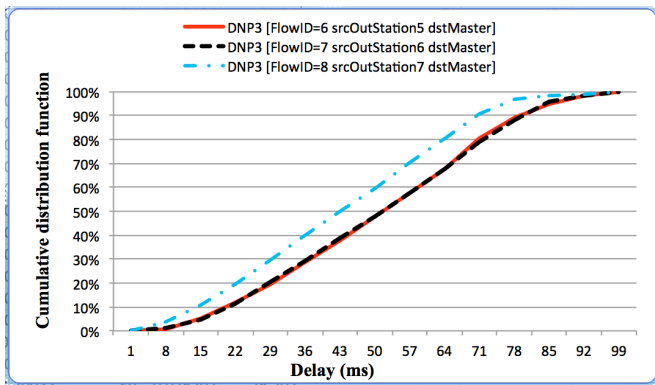


Fig. 8 Delay of Outstations of BS2 with TCP traffic.

Fig. 9 illustrates the delay in delivery of TCP traffic packages identified in red color of the node8 of substation1 resulting in a line with the time delay of 78 ms, the color identified with the blue Node9 of BS2 in form resulted in the delay time sine of 85 ms.

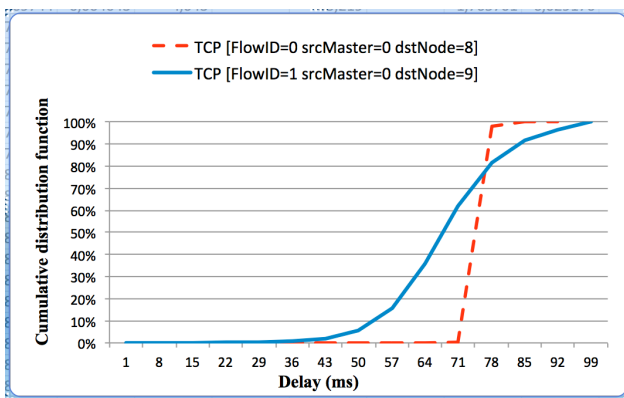


Fig. 9 Delay of node8 of substation1 and node9 of substation2.

#### IV. CONCLUSIONS

This work aimed to perform simulations in a scenario involving two substations and one control center. It is through the simulation scenario in NS-2 analyzing the performance and viability of the use of the DNP3 under TCP/IP in a mixed network with normal traffic and with heterogeneous traffic, using the FTP data traffic through the TCP transport protocol.

The results of the simulations showed that when the DNP3 used in a mixed network between IEEE 802.3 and IEEE 802.11b over TCP/IP even long distance are feasible for tele protection. The results of the delay was under 16 ms, the best case was obtained with the wired node reaching the delay time below 5ms, already with the wireless node was also obtained good results with time delay under 11 ms.

With heterogeneous traffic is infeasible to use for tele-protection, because the delay times were above 16 ms, but can be used for real-time monitoring and data acquisition of smart meters because the times obtained were below 100 ms around 91ms in case higher than forecast.

As future work is to be performed a simulation with mixed networks with heterogeneous traffic with QoS (quality of service), also using the WiMax network.

#### ACKNOWLEDGMENT

This study was supported by grants of Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP, 2014/06022-9), Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (bolsista da CAPES - Proc. n° 99999.002669/2014-05) and Universidade Estadual de Mato Grosso do Sul (UEMS).

#### REFERENCES

- [1] R. Hassan and G. Radman, "Survey on smart grid," in *IEEE Southeast-Con 2010 (SoutheastCon), Proceedings of the*, March 2010, pp. 210–213.
- [2] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid — the new and improved power grid: A survey," *Communications Surveys Tutorials, IEEE*, vol. 14, no. 4, pp. 944–980, Fourth 2012.
- [3] Zheng, D. Gao, and L. Lin, "Smart meters in smart grid: An over view," in *Green Technologies Conference, 2013 IEEE*, April 2013, pp. 57–64.
- [4] X. Lu, W. Wang, and J. Ma, "An Empirical Study of Communication Infrastructures Towards the Smart Grid: Design, Implementation, and Evaluation," *Smart Grid, IEEE Transactions on*, vol. 4, no. 1, pp. 170–183, March 2013.
- [5] Parikh, M. Kanabar, and T. Sidhu, "Opportunities and challenges of wireless communication technologies for smart grid applications," in *Power and Energy Society General Meeting, 2010 IEEE*, July 2010, pp. 1–7.
- [6] H. Kanchev, D. Lu, F. Colas, V. Lazarov, and B. Francois, "Energy management and operational planning of a microgrid with a PV-Based Active Generator for Smart Grid Applications," *Industrial Electronics, IEEE Transactions on*, vol. 58, no. 10, pp. 4583–4592, Oct 2011.
- [7] G. Clarke, D. Reynders, and E. Wright, *Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems*, 1st ed., ser. Engineering: instrumentation & control. Elsevier, 2004, no. pp. 66-164.
- [8] IEEE, "IEEE draft standard for exchanging information between networks implementing IEC 61850 and IEEE std 1815 (distributed network protocol - DNP3)," *IEEE P1815.1/D4.00*, June 2012, pp. 1-283, June 2012.
- [9] R.Lasseter,J.Eto,B.Schenkman,J.Stevens,H.Vollkommer,D.Klapp, E. Linton, H. Hurtado, and J. Roy, "CERTS Microgrid Laboratory Test Bed," *Power Delivery, IEEE Transactions on*, vol. 26, no. 1, pp. 325-332, Jan 2011.
- [10] A.Ortega and A.Akira Shinoda, "Simulation in NS-2 of DNP3 protocol encapsulated over TCP/IP in smart grid applications," in *Innovative Smart Grid Technologies Latin America (ISGT LA), 2013 IEEE PES Conference On*, April 2013, pp. 1–8.
- [11] A. Ortega, C. Schweitzer, and A. Akira Shinoda, "Performance analysis of smart grid communication protocol DNP3 over TCP/IP in a heterogeneous traffic environment," in *Communications and Computing (COLCOM), 2013 IEEE Colombian Conference on*, May 2013, pp. 1–6.
- [12] S. Bagaria, S. Prabhakar, and Z. Saquib, "Flexi-DNP3: Flexible distributed network protocol version 3 (DNP3) for SCADA security," in *Recent Trends in Information Systems (ReTIS), 2011 International Conference on*, Dec 2011, pp. 293–296.
- [13] IEEE, "IEEE standard for electric power systems communications-distributed network protocol (DNP3)," *IEEE Std 1815-2012*, pp. 1–821, Oct 2012.
- [14] X. Lu, Z. Lu, W. Wang, and J. Ma, "On Network Performance Evaluation toward the Smart Grid: A Case Study of DNP3 over TCP/IP," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, Dec 2011, pp. 1–6.